

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 04-181282
(43) Date of publication of application : 29.06.1992

(51) Int.Cl.

G09C 1/00
G06F 12/00
H04L 9/00
H04L 9/10
H04L 9/12

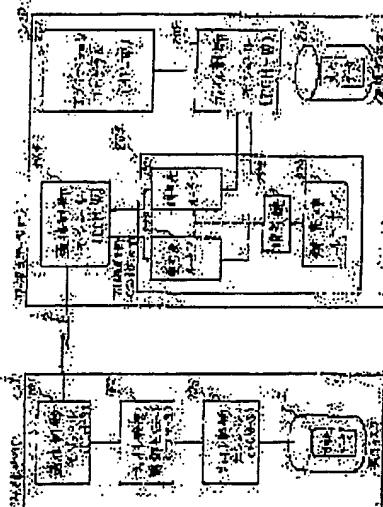
(21) Application number : 02-308893
(22) Date of filing : 16.11.1990

(71) Applicant : HITACHI LTD
(72) Inventor : ISHII YASUHIRO

(54) CRYPTOGRAPHIC SYSTEM FOR FILE

(57) Abstract:

PURPOSE: To enhance cryptogram processing efficiency by making data on a line and data on a file into the same ciphered data.
CONSTITUTION: A file server 1 has a communication control module 101, a file transfer control module 102, and a file control module 103, inside, and connected with an actual disc 3. A work station 10 has an application program 201, a file control module 202, a file transfer control module (FTM-W)203, and a communication control module 204, and the (FTM-W)203 has a ciphering routine 221, a decoding routine 222, a key control routine 223, and an cryptographic key 224. Further, the file server 1 and the work station 10 are connected by an LAN network 2. The ciphered data is housed in the actual disc 3 of the file server 1, and in a data transfer from the work station 10 to the file server 1 as well, safety is obtained with respect to tapping, etc., because the data is ciphered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑩ 日本国特許庁 (JP)

⑪ 特許出願公開

⑫ 公開特許公報 (A) 平4-181282

⑬ Int. Cl. 5

G 09 C 1/00
G 06 F 12/00
H 04 L 9/00
9/10
9/12

識別記号 廈内整理番号

537 H 7922-5L
8944-5B

⑭ 公開 平成4年(1992)6月29日

7117-5K H 04 L 9/00

Z
審査請求 未請求 請求項の数 3 (全6頁)

⑮ 発明の名称 ファイルの暗号方式

⑯ 特 願 平2-308893

⑰ 出 願 平2(1990)11月16日

⑱ 発明者 石井 保弘

神奈川県秦野市堀山下1番地 株式会社日立製作所神奈川
工場内

⑲ 出願人 株式会社日立製作所

東京都千代田区神田駿河台4丁目6番地

⑳ 代理人 弁理士 小川 勝男

外1名

明細書

1. 発明の名称

ファイルの暗号方式

2. 特許請求の範囲

1. 電子計算機を通信回線等を用いて接続し、各電子計算機で作成したファイルを接続された任意の電子計算機に保管するシステムにおいて、データ作成元の電子計算機でファイルに保管するデータを暗号化し、暗号化されたデータを通信回線等を使用して保管する電子計算機に送り、保管する電子計算機では暗号化されたデータをファイルとして保管することを特徴とするファイルの暗号方式。

2. 請求項(1)において、該保管先の電子計算機は通信回線等を使用して該暗号化されたデータをデータ作成元の各電子計算機に送り、各電子計算機はデータを暗号化してファイルの元の内容を替ることを特徴とするファイルの暗号方式。

3. 請求項(1)又は(2)において、データ暗

号をファイル使用者の暗号機にて暗号化して暗号化されたデータとともに保管先の電子計算機にて保管することを特徴とするファイルの暗号方式。

3. 発明の詳細な説明

【底盤上の利用分野】

本発明は電子計算機のファイルの保管方法に関するもので、特に、通信回線で接続された別の電子計算機にデータを暗号化して保管する方法に関するものである。

【従来の技術】

従来の暗号方式については暗号(コンピュータ:データ保護の新技術)第275ページから第306ページにおいて論じられている。

これによれば、回路暗号は送信する電子計算機同士が共通の暗号機を有し、この暗号機に従って回路に送出するデータを暗号化し、受信側は該暗号機により同様に復号化することになっている。

ファイル暗号はファイル対応にファイル個を生成し、この間に従ってファイル内データを暗号化することになっている。

ある電子計算機上のデータを他の電子計算機のファイルに安全に格納するためには次の処理が必要である。まず、回線暗号手順を用いて作成元電子計算機と接続電子計算機間で暗号通信を行い、データを安全に転送する。次に、ファイル暗号手順を用いて、データを暗号化してファイルに格納することとなる。

【発明が解決しようとする課題】

上記従来技術は、ファイルサーバ方式などのような通信回路を介してファイルをアクセスするファイル制御の暗号方式について記載されておらず、次のような問題点があつた。

(1) 回線上のデータ保護のために、ワークステーションからファイルサーバあるいはファイルサーバからワークステーションへのデータ送信の度に暗号暗号を行なう。また、ファイル保護のために、ファイルサーバに置いてファイルのデータの格納あるいはデータの読みだしの度にファイル暗号を行う必要がある。このように、回線暗号とファイル暗号を重複して行なう必要があり、処理効率が悪くなる。

これによれば、ワークステーションからファイルサーバへファイルを格納する場合、各ワークステーションは格納したいデータを自ワークステーション内で暗号化してファイルサーバに送信し、ファイルサーバは暗号化されたデータをそのままファイルに書き込み。

また、ファイルサーバからデータを読み取る場合、ファイルサーバは暗号化されたデータをファイルから読み込み、これをそのままワークステーションに送る。ワークステーションは自ワークステーション内で管理している暗号暗号で復号化し、データをそのままファイルに書き込む。

ゆえに、ワークステーションからファイルサーバあるいはファイルサーバからワークステーション間の通信データは暗号化されており、回線上の機密を保つことができる。また、ファイルサーバ内に格納されたデータも暗号化されており、ファイル上の機密を保つことができる。

このことより、ファイルサーバは機密/暗号処理をする必要がないので効率良く処理することができます。

い。

(2) 暗号管理室は機密上、システム管理者がファイルサーバ上で操作を行う必要がある。しかし、ファイルサーバの利用の利用形態からみて暗号ユーザが直接に行なうことは期待できない、故に、暗号管理室を簡素化する必要がある。

本発明は、このような問題点を解決するためになされたものである。

本発明の目的は、ファイルデータの暗号処理を効率よく行なうとともに、簡素な暗号管理室を提供することにある。

【課題を解決するための手段】

上記の目的を達成するために、各ワークステーションのみがファイルデータを暗号/復号化し、ファイルサーバは暗号化されたデータを直接ファイルに書き込み、あるいは、読みだしするようにしたものである。

また、暗号管理室も各ワークステーションで行なう。管理を局所化したものである。

【作用】

これによれば、ワークステーションからファイルサーバへファイルを格納する場合、各ワークステーションは格納したいデータを自ワークステーション内で暗号化してファイルサーバに送信し、ファイルサーバは暗号化されたデータをそのままファイルに書き込み。また、ファイルサーバは、暗号を行なないので暗号の管理は不要であり、暗号室がワークステーション内で閉じるので安全性が高まるとともに処理を簡素化することができる。

【実施例】

以下、本発明の一実施例を第1図、第2図により説明する。

第2図に電子計算機の接続図を示す。ファイルサーバ1は端末スカラを有し、LAN端子2に接続されている。ワークステーション10-15も接続されている。ワークステーション10-15は各ワークステーション内に接続されており、ファイルサーバ1と各ワークステーション10-15間は自由に通信できるようになっている。

第1図にファイルサーバ1とワークステーション10の接続構成図を示す。(ワークステーション1-15はワークステーション10と同一なのでここでは省略する。) ファイルサーバ1内には通信制御モジュール(CCM-S)101とファイル転送制御モジュール(FTM-S)102、ファイル制御モジュール(PCM-S)103。

0.3 があり、実ディスク3と接続されている。ワークステーション10内にはアプリケーションプログラム(AP-W)201とファイル制御モジュール(FCM-W)202、ファイル転送制御モジュール(FTM-W)203、および通信制御モジュール(CCM-W)204からなり。ファイル転送制御モジュール(FTM-W)203内は、暗号化ルーチン221と復号化ルーチン222、鍵管理ルーチン223、および、暗号鍵24からなる。ファイルサーバ1とワークステーション10はLAN網2にて接続されている。

次に書き込み時の処理手順について第3図を用いて説明する。

step301: アプリケーションプログラム(AP-W)201はファイル制御モジュール(FCM-W)202に対してライトモードでファイルのオープンを指示する。
step302: ファイル制御モジュール(FCM-W)202は仮想ディスク210上に仮想ファイルをアロケーションする。

204に蓋す。

step303: 通信制御モジュール(CCM-W)204は暗号化されたデータをファイルサーバ1に送る。
step310: 通信制御モジュール(CCM-S)101は暗号化されたデータを受け取り、ファイル転送制御モジュール(FTM-S)102に送る。
step311: ファイル転送制御モジュール(FTM-S)102はファイル制御モジュール(FCM-S)103に対してファイルのアロケーションを指示する。
step312: ファイル制御モジュール(FCM-S)103は実ディスク3上にファイルをアロケーションする。
step313: ファイル転送制御モジュール(FTM-S)102はファイル制御モジュール(FCM-S)103に対して暗号化されたデータの書き込みを指示する。
step314: ファイル制御モジュール(FCM-S)103は実ディスク3上に暗号化されたデータを

step303: アプリケーションプログラム(AP-W)201はファイル制御モジュール(FCM-W)202に対してデータの書き込みを指示する。

step304: ファイル制御モジュール(FCM-W)202は仮想ディスク上にデータを書き込む。
step305: アプリケーションプログラム(AP-W)201はファイル制御モジュール(FCM-W)202に対してファイルのクローズを指示する。

step306: ファイル制御モジュール(FCM-W)202はファイル転送制御モジュール(FTM-W)203に対して仮想ファイルをファイルサーバ1に転送することを要求する。

step307: ファイル転送制御モジュール(FTM-W)203は暗号化ルーチン222でファイルの暗号鍵を作成する。

step308: ファイルの転送制御モジュール(FTM-W)203は暗号化ルーチン223でファイルのデータを読み取り、暗号化ルーチン221で暗号し、通信制御モジュール(CCM-W)

書き込む。

これにより、ファイルサーバ1上の実ディスクには暗号化されたデータが格納される。また、ワークステーション10からファイルサーバ1へのデータ転送もデータが暗号化されているので盗聴などに対して安全である。

第4図にファイル読み取り処理手順について示す。

step401: アプリケーションプログラム(AP-W)201はファイル制御モジュール(FCM-W)202に対してリードモードでファイルをオープンする。

step402: ファイル制御モジュール(FCM-W)202はファイル転送制御モジュール(FTM-W)203に対してファイルサーバ1からのファイル転送を要求する。

step403: ファイル転送制御モジュール(FTM-W)203は通信制御モジュール(CCM-W)204および通信制御モジュール(CCM-S)101を介して、ファイル転送制御モジュール

(FTM-S) 102 に実ファイルの転送を指示する。

step404: ファイル転送制御モジュール (FTM-S) 102 はファイル転送モジュール (FCM-S) 103 に対してファイルの読み取りを指示する。

step405: ファイル転送モジュール (FCM-S) 103 は実ディスク 3 上の暗号化されたデータを読み取る。

step406: ファイル転送制御モジュール (FTM-S) 102 は通信制御モジュール (CCM-S) 101 に対して暗号化されたデータの転送を指示する。

step407: 通信制御モジュール (CCM-S) 101 はワークステーション 10 に暗号化されたデータを送信する。

step408: 通信制御モジュール (CCM-W) 204 は暗号化されたデータを受け取り、ファイル転送制御モジュール (FTM-W) 203 に渡す。

step409: ファイル転送制御モジュール (FTM-

-W) 203 は暗号化ルーティング 223 で暗号鍵 224 を設定する。

step410: ファイル転送制御モジュール (FTM-W) 203 は暗号化データを暗号化ルーティング 222 で元のデータに復元し、仮想ディスク 210 に元のデータを書き込む。

step411: アプリケーションプログラム (AP-W) 201 はファイル転送モジュール (FCM-W) 202 に対してファイルの読み取りを指示する。

step412: ファイル転送モジュール (FCM-W) 202 は仮想ディスク上のデータを読み取る。

step413: アプリケーションプログラム (AP-W) 201 はファイル転送モジュール (FCM-W) 202 に対してファイルのクローズを指示する。

step414: ファイル転送モジュール (FCM-W) 202 は仮想ディスク上のファイルを削除する。これにより、ワークステーション 10 上のアプリケーションプログラム (AP-W) 201 はフ

ァイルサーバ 1 の実ディスク 3 に転送されたデータを生のデータとして読み取ることができる。また、ファイルサーバ 1 からワークステーション 10 へのデータ転送もデータが暗号化されているので盗聴などに対して安全である。

また、暗号化ルーティング 223 で生成した暗号鍵 224 はファイル所有者のマスクで暗号化し、224 はファイル所有者のマスクで暗号化し、ファイルのヘッダとしてデータに添付し、実ファイル 8 に組み込んでおく。これにより、ファイルの読みだし時、ヘッダの暗号化された鍵を暗号化し、この暗号鍵 224 でデータを復号化することができる。鍵の管理をより簡単に保つことができる。

このように、本実施例によれば次の効果がある。
(1) 1 回の暗号処理で LAN 第 2 上のデータの暗号化と、ファイルサーバ 1 の実ディスク 3 上のデータの暗号化が可能であり、処理効率を高めることができる。

(2) ワークステーション 10 での暗号処理を行い、ファイルサーバ 1 では暗号処理を行わない。

ゆえに、鍵管理はワークステーション 10 ないに求めることができるので、鍵管理が飛躍的に簡単となる。

【発明の効果】

本発明に依れば、次の効果がある。

(1) 回線上のデータとファイル上のデータを同一の暗号化データとするので、回線暗号ヒファイナル暗号を 1 回の暗号処理で済ますことができるので、暗号処理効率を高めることができます。

(2) ファイル作成元でのみ暗号処理を行い、ファイル転送先では暗号処理を行わない。ゆえに、鍵管理を局所化できるので、鍵管理が飛躍的に簡単となる。

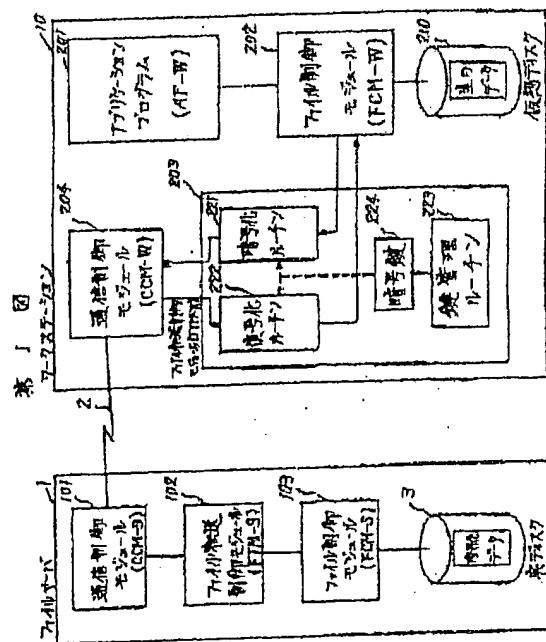
4. 図面の簡単な説明

第 1 図は本発明の一実施例であるシステムの処理ブロック図、第 2 図はシステムの構成図、第 3 図はファイル書き込み時の処理フロー図、第 4 図はファイル読み取り時の処理フロー図である。

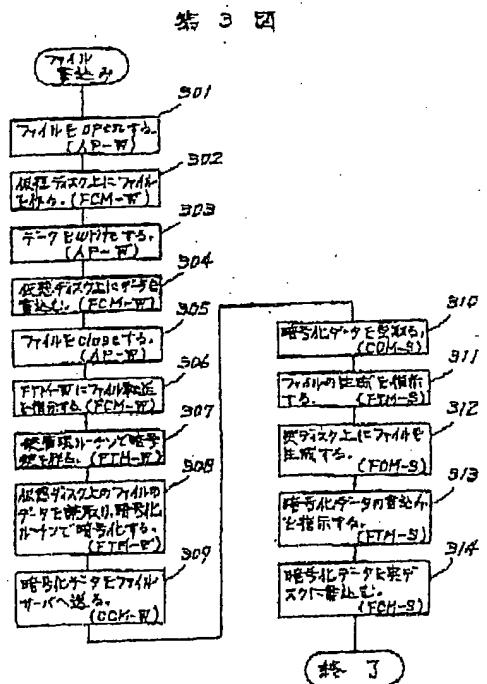
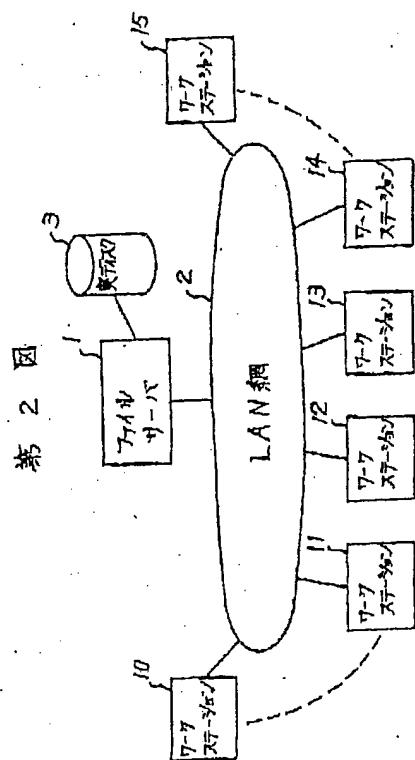
【符号の説明】

1 … ファイルサーバ、2 … LAN 線、3 … 実ディ

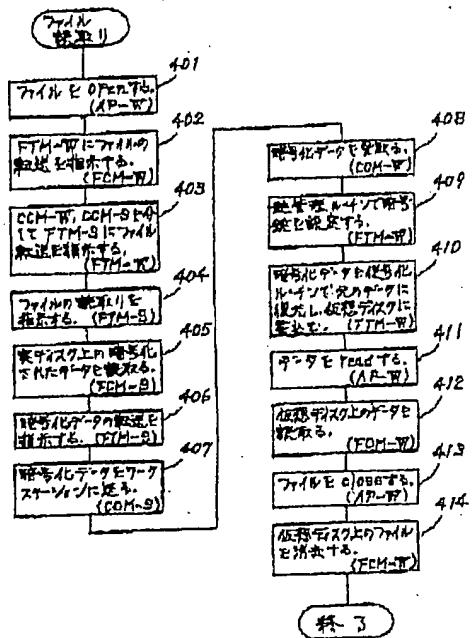
スク、10、11、12、13、14、15…ワ
ークステーション、101…通信制御モジュール
(CCM-S)、102…ファイル転送制御モジ
ュール(FTM-S)、103…ファイル制御モ
ジュール(FCM-S)、201…アプリケー
ションプログラム(AP-W)、202…ファ
イル制御モジュール(FCM-W)、203…ファ
イル転送制御モジュール(FTM-W)、204
…通信制御モジュール(CCM-W)、221…
信号化ルーチン、222…復号化ルーチン、22
3…統管取ルーチン、224…暗号集。



代理人弁理士 小川 勝男



第4 図



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.